U.S. E-Authentication Identity Federation Governance

Business Owner: Federation Management
Creation Date: 12/20/2006
Last Updated: 9/24/2007
Version: EA-PL-0098-1.0.3-F
Audience: Public

GSA

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.1	08/22/06	Initial content added.	Limited
Draft	0.0.2	08/24/06	Revised background section.	Limited
Draft	0.1.0	08/24/06	Submitted to PMO for review.	PMO
Draft	0.2.0	08/28/06	Revisions per PMO review.	PMO
Draft	0.2.1	08/30/06	Revisions per working group meeting	Limited
Draft	0.3.0	08/30/06	Submitted to PMO for review.	PMO
Draft	0.3.1	08/31/06	Revisions based on comments from the PMO.	Limited
Draft	0.4.0	08/31/06	Submitted to PMO for review.	PMO
Draft	0.4.1	09/05/06	Added purpose and scope content and additional authoritative documents.	Limited
Draft	0.5.0	09/06/06	Submitted to PMO for review.	PMO
Draft	0.5.1	09/11/06	Made revisions based on RP and CSP Member Council meeting.	Limited
Draft	0.5.2	09/21/06	Made revisions based on comments received.	Limited
Draft	0.6.0	09/22/06	Submitted to PMO for review.	PMO
Draft	0.6.1	10/06/06	Made revisions based on comments received.	Limited
Draft	0.6.2	10/12/06	Revisions based on comments from the PMO.	Limited
Draft	0.6.3	10/17/06	Made revisions based on comments received.	Limited
Draft	0.7.0	10/19/06	Submitted to PMO.	PMO
Draft	0.7.1	11/20/06	Made revisions based on LWG comments.	Limited
Draft	0.8.0	12/05/06	Submitted to PMO.	PMO
Draft	0.8.1	12/20/06	Revisions per working group meeting.	Limited
Public	1.0.0	12/21/06	Distributed to Legal WG and EAuth ESC	
Draft	1.0.1	7/9/07	Revisions necessitated by Architecture 2.0	Limited
Draft	1.0.2	9/15/07	Revisions per PMO comment	Limited
Draft	1.0.3	9/24/07	Revisions per PMO comment	Limited

Editors

Georgia Marsh	Myisha Frazier-McElveen	Doug Hansen
Cassandra Bonnette	Dave Silver	Chris Broberg
Kendra Brown	Steve Lazerowich	

Table of Contents

1 INTRODUCTION

1.1 Purpose and Scope

Governance, as defined herein, ensures that the best interests of the overall U.S. E-Authentication identity Federation (Federation) are maintained. This document improves the internal management of the Federal Government by defining governance structure, Federation change management, waivers, dispute resolution, and business standards.

This document does not confer any benefits or impose any obligations on the public. It does not create any right or benefit, substantive or procedural, enforceable at law by a party against the Relying Party (RP), Credential Service Provider (CSP), the E-Authentication Program Management Office (E-Auth PMO), their officers, employees or agents, the Federal Government or the public. It does not obligate nor does it require any agency to obligate any agency appropriations. The sole and exclusive remedy for any failure on the part of a government agency to carry out its responsibilities under this document will be the withdrawal of its authority to participate in the Federation.

1.2 References

This document uses National Institute of Standards and Technology (NIST) convention for citing documents. The shorthand format *[Doc Reference]* represents the document referenced in this section. For example, [CAF] is a shorthand reference that refers back to this section's full citation for the *Credential Assessment Framework* document.

[CAF] Credential Assessment Framework
http://www.cio.gov/eauthentication/CredSuite.htm

[Escalation Plan] Federation Escalation Plan
Available from the PMO

[Federal Register] Federal Register, Vol. 70, No. 150 / Friday, August 5, 2005 / Notices, 45392-45394
http://www.access-board.gov/ada-aba/corrections.pdf

[Federation Governance] E-Authentication Federation Governance
http://www.cio.gov/eauthentication/MembershipDocuments.htm

[Federation Standards] E-Authentication Federation Operational Standards
http://www.cio.gov/eauthentication/MembershipDocuments.htm

[Financial Privacy Act] Right to Financial Privacy Act of 1978; Codified to 12 U.S.C. 3401
http://www.fdic.gov/regulations/laws/rules/6500-2550.html

[Joining the Federation] Joining the E-Authentication Federation
http://www.cio.gov/eauthentication/

[NIST SP 800-63] Electronic Authentication Guideline, National Institute of Science and Technology (NIST Special Publication 800-63)
http://csrc.nist.gov/publications/nistpubs/

[OMB M-04-04]	E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) Memorandum M-04-04 http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf
[Style Guide]	U.S. E-Authentication Identity Federation Style Guide Available from the PMO
[Tech Approach]	Technical Approach for the Authentication Service Component http://www.cio.gov/eauthentication/TechnicalArchitecture.htm
[Tech Suite]	E-Authentication Technical Architecture http://www.cio.gov/eauthentication/TechnicalArchitecture.htm

1.3 Background

In 2002, the Office of Management and Budget (OMB) designated the General Services Administration (GSA) as the lead agency for the E-Authentication Initiative (Initiative), a cross-cutting initiative of the E-Government component of the President's Management Agenda. The Initiative was charged with developing a means of defining the levels of risk associated with online transactions performed between the public and government or between government entities, and to make available a set of common solutions to mitigate that risk.

With the approval of its Executive Steering Committee (ESC), and a governance body comprised of representatives of the twenty-four (24) Chief Information Officer (CIO) Council agencies, the Initiative elected to pursue a federated approach to identity management to provide a standardized, government-wide means of authenticating End- Users of online government services, thereby reducing the risk to E-Government. The result was the creation of the Federation, a public-private partnership that enables citizens, businesses and government employees to access online government services using Credentials issued by trusted third-parties, both within and outside the government.

Government agencies may bring into the Federation any Internet-based System that has End-Users outside the agency's firewall and requires identity verification of those End-Users. Once an agency's System has been E-Authentication-enabled, it will be able to grant access to End-Users who have an identity Credential from one or more of the Federation's CSPs. If End-Users do not already have a Credential from an Approved CSP, they may obtain an Approved Credential that will be usable to gain access to multiple Federation Member services.

The Authentication Service Component (ASC) provides the operational infrastructure of the Federation. The ASC is a recognized component of the Federal Enterprise Architecture (FEA) and, as such, is the recommended technical approach for online End-User authentication for Federal agencies.

The ASC does not create or maintain any new Federal System of Records, but does provide for the authorized exchange of information among systems of records that have been or will be established to support Federal E-Government programs and services.

The Federation is managed by the E-Auth PMO in the Federal Acquisition Service of GSA. The Federation follows [OMB M-04-04], which provides policy guidance for identity authentication, and [NIST SP 800-63], which is the technical companion document to [OMB M-04-04]. The GSA Office of Government-wide Policy (OGP) provides policy support for the Federation.

1.3.1 *Federation Members*

Federation Members are business or government organizations that sign an agreement with the E-Auth PMO to participate in the Federation. Section 1.3.3 describes those Federation Member Systems.

The E-Auth PMO authorizes an organization's participation in the Federation. Once authorized, the organization becomes a Federation Member and is added to the Federation Membership List[1]. The process for becoming a Federation Member is described in [Joining the Federation]. Currently, Federation Members include:

- ***Credential Services Providers (CSPs)*** – Organizations (commercial or government) that provide the Federation with identity management services.
- ***Relying Parties (RPs)***[2] – A department, agency, government sponsored corporation, or other government organization, or any state or local government that provides online services requiring End-User authentication.

Federation Members are obligated to comply with all applicable Federation standards, requirements, policies, procedures, and related materials defined by the E-Auth PMO that govern participation in the Federation.

1.3.2 *Authentication Service Component*

The ASC is a common infrastructure for electronically authenticating the identity of End-Users of E-Government services[3]. The ASC accomplishes this by leveraging Credentials from multiple CSPs through certifications, guidelines, standards adoption and policies – which is the basis of trust for Federation Credentials. In addition, the ASC supports varying levels of identity assurance (i.e., levels of confidence). Federation Members do not need to support every identity level of assurance. The ASC's broad range of authentication services makes separate credentialing by an RP unnecessary.

Currently, the ASC supports two architectural techniques for identity authentication within the same environment:

- **Assertion-based Authentication** – Personal Identification Number (PIN) and Password based authentication, where End-Users authenticate to a selected Credential Service (CS), which in turn asserts the End-User identity to the appropriate RP. An example of Assertion-based Authentication supported by the ASC is *Security Assertion Markup Language (SAML) 2.0 Single Sign-on (SSO) Profile Using HTTP POST*[4].
- **Certificate-based Authentication** – X.509v3 digital certificate based authentication in a public key infrastructure (PKI). Certification Authorities (CAs) issue certificates to End-Users, and End-Users present their certificates to applicable RPs for authentication.

The E-Auth PMO may adopt additional identity authentication techniques over time, as necessary to serve the best interests of the Federation.

---

[1] http://www.cio.gov/eauthentication/documents/FederationMemberList.pdf

[2] Per identity management industry convention, RP can refer to both the organization that provides an online system needing authentication service and the online system itself. The Federation uses RP to mean both.

[3] [Federal Register]

[4] [Tech Approach]

Currently, the ASC comprises the following:

- ***E-Auth PMO-provided Components*** – subsystems that support the design goals[5] and operation of the Federation. This may include, but is not limited to a Federation Portal, scheme translators, Federation Domain Name Service (DNS), and certificate-based validation services.

E-Auth PMO-provided components must abide by the Federal Information Security Management Act (FISMA) and GSA security policies and procedures, including GSA Information Technology (IT) Security Policy, and Certification and Accreditation (C&A).

1.3.3 Federation Member Systems that Integrate into the ASC

The ASC is a framework into which Approved Federation Member Systems integrate, in accordance with applicable interface specifications and procedures. Once integrated, Federation Member Systems technically interoperate with other Federation Member Systems and/or E-Auth PMO-provided components as necessary to authenticate End-Users. Currently, the E-Auth PMO integrates the following types of Federation Member Systems into the ASC:

- ***Relying Parties (RPs)***[6] – Federation Member Systems (Internet based) that take an action based on identity information from a trusted Federation Member System (e.g., a SAML assertion from a CS, a PKI certificate issued by a CA). RPs are required to manage all Business Transactions and all End-User authorization decisions.[7]
- ***Credential Services (CSs)***[8] – Federation Member Systems that create, maintain, and manage identity information for End-Users, and may provide End-User authentication to RPs. A CS is a CA when it issues PKI certificates for use by the Federation.

1.3.4 Program Management Office

The E-Auth PMO manages the Federation on an ongoing, day-to-day basis. This includes but is not limited to the following:

- Defining policies and guidelines for Federal authentication;
- Defining processes for determining the qualification of any party in the Federation;
- Defining technical architecture and providing documents, including Interface Specifications, for communications within the ASC;
- Defining standards and governance for operating within the Federation;
- Defining Change Management processes for the Federation;
- Conducting credential assessments and authorizations;
- Conducting interoperability testing of candidate products, schemes or protocols;
- Providing Management and control of accepted Federation schemes operating within the ASC;
- Providing Quality management of the Federation; and
- Facilitating the roles, relationships and mutual obligations of all parties operating in the Federation.

---

[5] Standards based, use of commercial off the shelf products, federation, durability, and flexibility; [Tech Approach]

[6] The identity management industry also calls this a 'Service Provider' (SP)

[7] Business Transactions and all End-User authorization decisions are outside the scope of the ASC.

[8] The identity management industry calls this an 'Identity Provider' (IdP)

2 FEDERATION GOVERNANCE

2.1 Governance Structure

The E-Auth PMO governs the Federation on a day-to-day basis. It receives strategic direction from the E-Authentication ESC, and feedback from various boards, councils, and groups. The Technical Working Group (TWG) provides the E-Auth PMO with technical architecture, interface specification, and technology recommendations and documents. Figure 2-1 depicts the Federation governance structure. Table 2-1 profiles each governance entity.

Figure 2-1: Federation Governance Structure

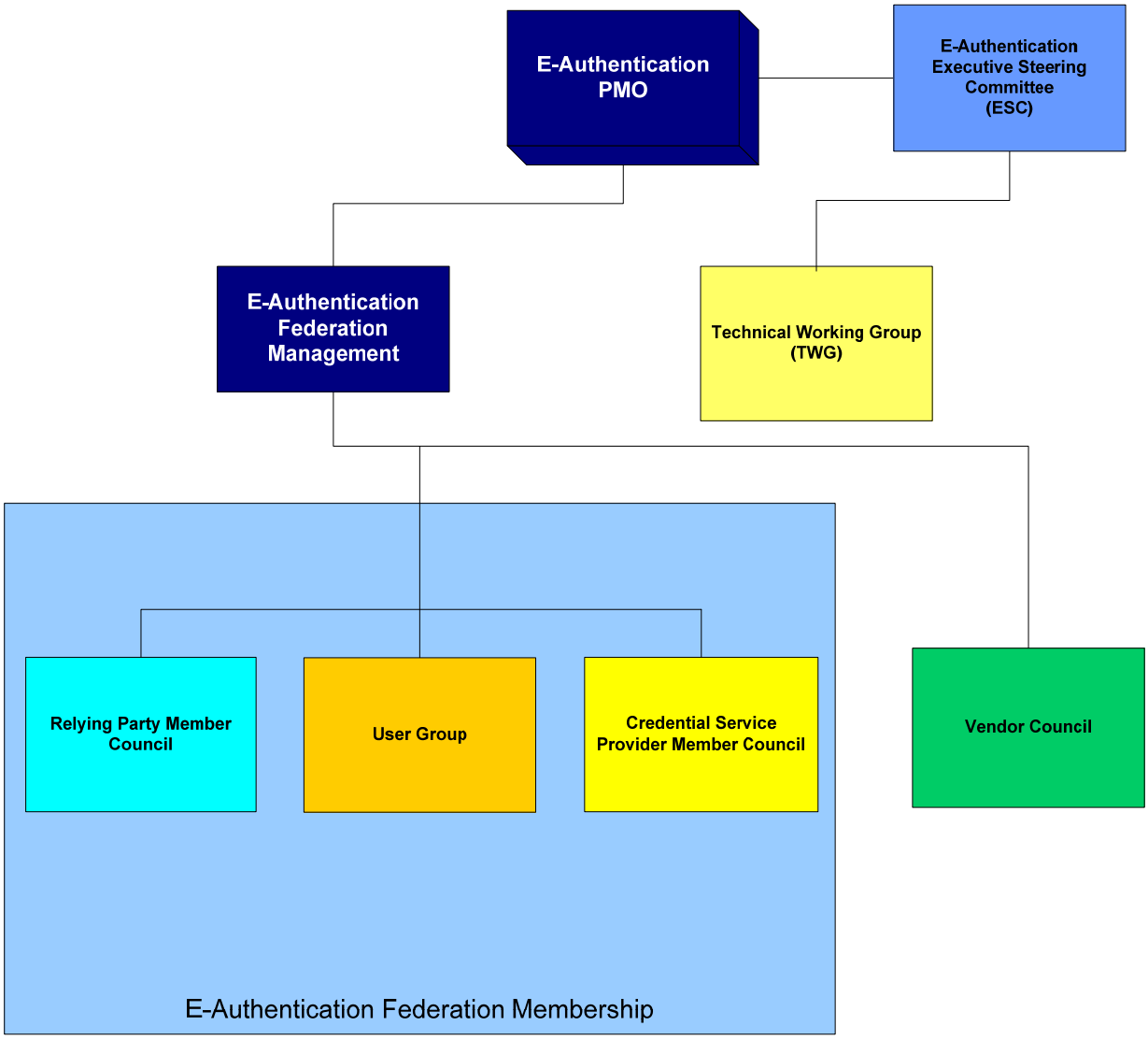

Table 2-1: Federation Governance Entities

Entity	Chair	Membership	Role	Decision-Making
Executive Steering Committee (ESC)	Elected ESC Member	Cabinet-level Agency CIO or CIO designee.	Advisory and oversight responsibility for the E-Authentication Initiative including guidance on strategy and approval of the Initiative's business, spend, and funding plans. In addition, makes final decision when E-Auth PMO cannot resolve a dispute with a Federation Member.	Majority vote
E-Authentication Program Management Office (PMO)	Appointed by GSA	Program Executive (PE), Deputy Program Manager (PM), and staff.	Responsible for Federation management, operations, management of products/services, and acquisition services, plus project management functions such as communications, reporting, budget, Change Management, and architecture.	Program Executive
Federation Management	Federation Manager	Staff	Responsible for day to day Federation management and administration, outreach and recruitment of commercial CSPs and strategic E-Government applications, relationship management of relying parties and CSPs, maintenance of associated Federation documents, formation and management of Federation boards/groups/councils, Change Management, ensuring ongoing security and privacy of the Federation, and Federation membership compliance.	Federation Manager

Entity	Chair	Membership	Role	Decision-Making
Credential Service Provider (CSP) Member Council	Elected by the membership	One designated representative for each CSP Federation Member System.	Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management regarding issues and Changes impacting CSPs including Federation standards and requirements, E-Authentication architecture and technical specifications, current or potential schemes, the Credential Assessment Framework (CAF), the Federation membership System, and other business and operations policies. Subcommittees may be created as necessary to address specific issues or proposed Changes.	None
Relying Party (RP) Member Council	Elected by the Federation Manager	One designated representative for each RP Federation Member System.	Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management regarding issues and Changes impacting RPs including Federation standards and requirements, E-Authentication architecture and technical specifications, current or potential schemes, the Federation membership System and other business and operations policies. Subcommittees may be created as necessary to address specific issues or proposed Changes.	None
Vendor Council	Appointed by the E-Auth PMO	Representatives of vendors with Approved products within the ASC.	Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management on issues or Changes impacting vendors and/or relative to commercial-off-the-shelf (COTS) electronic authentication products.	None

Entity	Chair	Membership	Role	Decision-Making
Federation User Group	Appointed by the Federation Manager	One or more representatives for each Federation Member.	Responsible for providing input and recommendations (either solicited or unsolicited) to Federation Management on issues or Changes impacting Federation Member End-Users. Subcommittees may be created as necessary to address specific issues or proposed Changes.	None
Technical Working Group (TWG)	Appointed by the E-Auth PMO	Technical subject matter experts recommended by an ESC representative or the E-Auth PMO.	Responsible for making E-Authentication architectural and technical specification recommendations to the ESC and the E-Auth PMO, at the request of the ESC, E-Auth PMO or Federation Chief Architect.	None

2.2 Federation Change Management

The Federation Change Management Process (FCMP)[9] ensures standard methods and procedures are used to minimize and manage risks with the lowest impact on service quality. The main goal of FCMP is to ensure there is appropriate communication of Change events and to provide a process that protects the Federation from Changes that are potentially disruptive, in conflict or of unacceptable risk. Change Management is the process of communicating, coordinating, scheduling, and monitoring Change to the E-Authentication infrastructure and resources. Additionally, Change Management provides a high level of availability and service to the Federation.

The Federation defines Change as "to make different, alter, or modify." Changes include, but are not limited to the following:

- Architectural Changes
  - Vendor Product Upgrades or Version Changes
  - Authentication Schema Changes
  - Metadata Information
- System Relocation Changes
  - DNS or Uniform Resource Locator (URL) Changes
- Point of Contact Information Changes

The E-Auth PMO has determined that establishment of the FCMP is critical for sustaining a world class operation and approach that (a) consists of several key steps to ensure consistency in communication, evaluation, and management, and (b) mitigates Change-related risks over time.

In addition, the FCMP is complementary to the configuration or change management processes each Federation Member has already established within their current operations. It is the responsibility of each Federation Member to evaluate any potential Changes that may have an adverse impact on the performance and availability of their E-Auth Applications and other Federation Member Systems. Notification of Changes having an adverse impact should be forwarded to the E-Auth PMO via the E-Auth Helpdesk.

Additionally, the E-Auth PMO internally implements best-practices for Change Management which provides Federation Members with the following:

1. Awareness and assurance that the Federation is operating appropriately;
2. Assurance that all Changes are controlled, carefully reviewed, and approved; and
3. Assurance that risks to service, reputation, and ongoing operations are identified, considered, and minimized.

The FCMP uses the following activities to manage Federation Changes:

- **Recording** – ensure that all sources of Changes can submit Change proposals and that they are recorded adequately;
- **Acceptance** – filter the Change proposals and accepting them for further consideration;
- **Classification** – determine the priority and impact of Changes on the risk to services and the availability of resources;
- **Planning and Approval** – consolidate, plan and approve Changes utilizing the Change Control Board (CCB). CCB membership is flexible and includes representatives from the Federation;

[9] Available at http://www.cio.gov/eauthentication/

- **Coordination** – coordinate building, testing, and implementation of the Change; and
- **Evaluation** – determine if each Change was successful and document learning lessons to improve the process.

Proposed changes may originate from any source, but should be sponsored by GSA, OMB, or a Federation Member to be considered. Change notifications are first submitted to the E-Auth PMO Change Manager. The Change Manager filters, accepts and classifies all Changes. The Change Manager evaluates the Change proposal and schedules it for CCB review. The CCB assesses and compiles resulting recommendations and provides them to all interested parties. Classification of the Change proposal determines the timeframe to implement the Change and to comply in the production environment. Federation Members and the E-Auth PMO implement Changes in accordance with the agreed-upon implementation plans, as documented in the Change proposal. A full description of the Change process is provided in the Federation Change Management Process and Procedures document.

2.3 Governance and Operational Standards Waivers

While each Federation Member is expected to comply with all applicable governance and Operational Standards, there may be times when a Federation Member cannot comply with certain standards due to technical, operational, or other limitations. In this case, the Federation Member may request a waiver. The following governs the waiver process:

- Federation Members submit waiver requests to the E-Auth PMO via the Waiver Request Form, which is available from the E-Auth PMO;
- The Federation Manager approves or denies waiver requests;
- The Federation Manager ensures that no waiver materially affects Federation security and operational integrity – a critical input to determining whether a waiver request should be approved;
- No permanent waivers are granted;
- The Federation Manager shares approved waivers and supporting material with all Federation Members connected to the System of the Federation Member receiving the waiver;
- A Federation Member can initiate a dispute regarding a denied waiver by providing the E-Auth PMO with a letter that includes the rationale for the dispute;
- The PE or the Deputy PM resolves disputes pertaining to waiver denials; and
- If the PE or the Deputy PM cannot resolve a dispute, the final decision is made by the ESC.

2.4 Dispute Resolution

2.4.1 Disputes amongst Federation Members

From time to time, Federation Members may have disputes amongst themselves. The dispute may pertain to a technical, operational, security, or other issues. To ensure compliance with standards and harmony within the Federation, the E-Auth PMO facilitates dispute resolution. The following governs Federation Member dispute resolution:

- Federation Members contact the Federation Manager regarding any dispute or concern pertaining to other Federation Members;
- The Federation Manager may initiate an investigation based upon the request of any Federation Member, or from any source, regarded as relevant and credible;
- The E-Auth PMO responds to every request to investigate a dispute in a timely manner;
- The E-Auth PMO immediately notifies appropriate Federation Members that they are the subject of an investigation;

- The E-Auth PMO may request additional information from one or more parties to the dispute;
- Upon determining that one or more Federation Members are not in compliance with standards and requirements, the E-Auth PMO takes appropriate action, in accordance with Federation standards, requirements, and signed agreements;
- The E-Auth PMO provides adequate notice to Federation Members regarding actions to be taken regarding the Federation Members;
- The E-Auth PMO may require additional audit, re-approval or approval at different Assurance Level(s), to the extent necessary to prevent or limit serious harm to the Federation; and
- Federation Members have the right to appeal any proposed suspension, in accordance with the E-Auth PMO violation procedures. Additional information is provided in the Member Violation Process document.

2.4.2 Disputes between Federation Members and the E-Auth PMO

From time to time, a dispute may arise between one or more Federation Members and the E-Auth PMO. The dispute may pertain to a technical, operational, security, policy, procedure, or other issue. To ensure efficient resolution, the following procedures govern E-Auth PMO – Federation Member dispute resolution:

- The Federation Member(s) informs the Federation Manager of their dispute with the E-Auth PMO;
- The Federation Manager initiates appropriate discussions, research, and/or investigations, as necessary, to determine facts and formulate a response;
- The Federation Manager informs the Federation Member(s) of the E-Auth PMO's response; and
- If the dispute cannot be resolved, the final decision is made by the ESC.

3 BUSINESS STANDARDS

In addition to the Operational Standards and requirements presented above, Federation Members and the E-Auth PMO must abide by the Business Standards presented in this section, which are non-technical practices for Federation operations. These Business Standards pertain to security practices, communication amongst Federation Members and the E-Auth PMO, style guidelines, and authoritative documentation.

3.1 Security

3.1.1 Sensitive Information

All Federation Member personnel who have access to, or are authorized to work on Systems/devices processing or storing, End-User data must be screened via an individual background investigation that includes financial and criminal record checks[10].

3.1.2 Policies and Procedures

The E-Auth PMO, or its authorized representatives, will have the right to perform a review of Federation Member's relevant security, business continuity, data center and operations controls (at E-Auth PMO's own expense)[11].

In addition, Federation Members must mitigate against known vulnerabilities on Systems providing services to the Federation. Acceptable mitigation may consist of active remediation (e.g., patches, coded updates, firewall Changes). Please reference documents in Section 3.4, Authoritative Documents, for complete details.

3.1.3 Incident Response

This section defines incident management requirements. An incident is an event that affects a Federation Member System or service including, but not limited to, the following:

- Unwanted disruption or denial of service (DOS);
- Site performance or availability;
- The unauthorized use of a System for the processing or storage of data;
- Unauthorized Changes to System hardware, firmware, or software characteristics; or
- Security breaches to a Federation Member System.

All Federation Members are responsible for reporting any known incident that may affect the Federation promptly to the E-Auth PMO helpdesk (eauth.service.help@gsa.gov) and according to the E-Authentication Escalation Plan.

3.1.4 End-User Confidentiality

End-User confidentiality is a high priority for the Federation. Federation Members must protect End-User confidentiality at all times.

Approved CSPs and RPs may not share Personally Identifiable Information (PII) of an End-User, including any PII contained in a certificate or other identity assertion included in the Interface Specification, for the purpose of carrying out an Approved Party's responsibilities under documents

[10] Survivable Standard.

[11] Survivable Standard.

governing its participation in the Federation, unless the End-User has provided prior authorization in accordance with applicable law for the sharing of this information, or sharing the End-User's PII is otherwise permitted by applicable law.

Nothing herein governs the disclosure or use of an End-User's PII by an Approved CSP or RP for a purpose other than carrying out an Approved Party's responsibilities under documents governing its participation in the Federation. However, any such disclosure or use is subject to the restrictions of any applicable law.

Prior to providing an Approved Credential to an End-User, an Approved CSP must inform the End-User about the End-User's responsibility for maintaining the security of the Approved Credential, including any Token housing the Approved Credential, and for reporting to the CSP any known or reasonably suspected compromise of such Credential or Token to protect the Credential or Token from compromise.

Any financial institution as defined in [Financial Privacy Act] must comply with the [Financial Privacy Act] in providing CSP services as provided in the documents governing participation in the Federation. Specifically, a participating financial institution must (a) provide any required [Financial Privacy Act] notice to an End-User, including informing each End-User of the categories of information that will be disclosed to a government authority as defined in [Financial Privacy Act] for use as part of the End-User's participation in this program, and (b) obtain a [Financial Privacy Act] -compliant consent from the End-User where required to disclose that information to the government authority. These requirements apply whether the financial institution is acting on its own or on behalf of a government agency.

Before providing an Approved Credential, every Approved CSP must obtain the affirmative authorization of the End-User required by this section and an affirmative manifestation of assent by each End-User of the terms and conditions applicable to the use of the Approved Credential. In the case of organizational End-Users, all relevant rights and obligations, including notice requirements and requirements for authorization must pass through to each natural person acting on behalf of End-User within the Federation.

3.2 Communication

3.2.1 Support Services

The E-Auth PMO shall provide telephone support to assist in identifying and resolving service problems and in answering questions related to the operational use of the services.

The E-Auth PMO shall make technical support personnel available from 6:00 a.m. to 9:00 p.m. (ET) Monday through Friday to assist with identifying and resolving problems.

The E-Auth PMO shall provide emergency support for Federation components on a continuous basis to solve problems that render the Federation inoperable to End-Users or impairs their functionality.

3.2.2 Points of Contact

CSPs must have on-call personnel available after normal business hours for responding to emergency situations.

RPs must have on-call personnel available after normal business hours for responding to emergency situations where appropriate.

Federation Member contact information must be provided to the E-Auth PMO, who may provide it to Connected Members.

The E-Auth PMO will contact the Federation Member’s technical contacts via telephone, pager, and email whenever an incident occurs.

3.2.3 Reporting

The E-Auth PMO will maintain an email address that will allow Federation Members to submit reports.

Assertion-based RPs must provide a monthly report to the E-Auth PMO containing a list of assertion validations (success and failure) by CS.

Assertion-based CSPs must provide a monthly report to the E-Auth PMO containing a list of assertion validations (success and failure) by RP.

Certificate-based RPs must provide a monthly report to the E-Auth PMO containing certificate validations (success and failure) by CS unless utilizing the Federation validation service.

The E-Auth PMO must be notified of any proposed modifications that may negatively impact a Federation Member's interoperability or overall security posture at least thirty (30) days prior to implementation.

Federation Members must submit a report each quarter to the E-Auth PMO attesting they have conducted vulnerability scanning and have or are addressing all identified vulnerabilities. Federation Members must also attest that the identified vulnerabilities will not impact the security posture of the Federation.

3.3 Style Guidelines, Branding, and Logos

The E-Auth PMO will establish and maintain Federation approved content and information, which will be provided to Federation Members for use on their web sites, during press releases and interviews, and for use with other non-web media.

Federation Members must use and display the Federation logo as required by the [Style Guide].

3.4 Authoritative Documents

The E-Auth PMO requires Federation Members to comply with authoritative documents as applicable. The E-Auth PMO determines compliance with authoritative documents via different means, as appropriate. This includes, but is not limited to assessments, tests, audits, and checklists. The list of authoritative documents (or document suites) includes, but is not limited to the following:

Authoritative Document	Pertains To
The Credential Assessment Framework Suite	CSP
The Technical Suite	CSP, RP
E-Authentication Federation Operational Standards	CSP, RP
E-Authentication Federation Governance	CSP, RP
Federation Escalation Plan	CSP, RP
FIPS 140-2 – Security Requirements for Cryptographic Modules	CSP, RP
FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems	Federal CSP, Federal RP
FIPS200 - Minimum Security Requirements for Federal Information and Information Systems	Federal CSP, Federal RP
NIST SP 800-18 - Guide for Developing Security Plans for Federal Information Systems	Federal CSP, Federal RP
NIST SP 800-26 - Guide for Information Security Program Assessments and System Reporting Form	Federal CSP, Federal RP
NIST SP 800-30 - Risk Management Guide for Information	Federal CSP, Federal RP

Authoritative Document	Pertains To
Technology Systems	
NIST SP 800-37 - Guide for the Security Certification and Accreditation of Federal Information Systems	Federal CSP, Federal RP
NIST SP 800-47 - Security Guide for Interconnecting Information Technology Systems	Federal CSP, Federal RP
NIST SP 800-53 - Recommended Security Controls for Federal Information Systems	Federal CSP, Federal RP
NIST SP 800-60 - Guide for Mapping Types of Information and Information Systems to Security Categories	Federal CSP, Federal RP
NIST SP 800-63 - Electronic Authentication Guideline: Recommendations of the National Institute of Standards and Technology	CSP, RP
ISO/IEC 17799:2005 - International standard specifies requirements for establishing, implementing and documenting information security management systems (ISMS)	Commercial CSP
ISO/IEC 27001 - International standard that provides a specification for ISMS and the foundation for third-party audit and certification	Commercial CSP
SAS 70 - Guide that defines the standards an auditor must employ in order to assess the contracted internal controls of a service organization.	CSP, RP
CIO IL-Security-06-02 - Safeguarding Personally Identifiable Information	Federal CSP, Federal RP
CIO-IT Security-01-02 - Handling IT Security Incidents	Federal CSP, Federal RP
CIO-IT Security-04-25 - Windows 2003 Server Hardening	Federal CSP, Federal RP
CIO-IT Security-04-26 - FISMA/POA&M Implementation	Federal CSP, Federal RP
CIO-IT Security-06-29 - Contingency Plan Testing	Federal CSP, Federal RP
OMB Circular No. A-130 - Management of Federal Information Resources	Federal CSP, Federal RP
M-04-04 - E-Authentication Guidance for Federal Agencies	Federal RP
M-06-15 - Safeguarding Personally Identifiable Information	Federal CSP, Federal RP
M-06-16 - Protection of Sensitive Agency Information	Federal CSP, Federal RP

** Authoritative documents marked as CSP and/or RP, pertain to both Federal and Commercial CSPs and/or RPs.*

Appendix A: Acronyms

Acronym	Definition
ASC	Authentication Service Component
CA	Certification Authority
CAF	Credential Assessment Framework
CCB	Change Control Board
CIO	Chief Information Officer
COTS	Commercial-off-the-Shelf
CS	Credential Service
CSP	Credential Service Provider
C&A	Certification and Accreditation
DOS	Denial of Service
DNS	Domain Name Service
E-Auth PMO	E-Authentication PMO
ET	Eastern Time
ESC	Executive Steering Committee
FCMP	Federation Change Management Policy
FEA	Federal Enterprise Architecture
FISMA	Federal Information Security Management Act
GSA	General Services Administration
IT	Information Technology
NIST	National Institute of Standards and Technology
OGP	Office of Government-wide Policy
OMB	Office of Management and Budget
PE	Program Executive
PII	Personal Identifiable Information
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PM	Program Manager
RP	Relying Party
SAML	Security Assertion Markup Language
TWG	Technical Working Group
URL	Uniform Resource Locator